Vendor Analysis

Vendor Analysis: LexisNexis® Risk Solutions

KYC/AML Data Solutions, 2022

Chartis

Independent. Insightful. Actionable.

About Chartis

Chartis Research is the leading provider of research and analysis on the global market for risk technology. It is part of Infopro Digital, which owns market-leading brands such as Risk and WatersTechnology. Chartis' goal is to support enterprises as they drive business performance through improved risk management, corporate governance and compliance, and to help clients make informed technology and business decisions by providing in-depth analysis and actionable advice on virtually all aspects of risk technology. Areas of expertise include:

- Credit risk.
- Operational risk and governance, risk management and compliance (GRC).
- Market risk.
- Asset and liability management (ALM) and liquidity risk.
- Energy and commodity trading risk.
- Financial crime, including trader surveillance, anti-fraud and anti-money laundering.
- Cyber risk management.
- Insurance risk.
- Regulatory requirements.
- Wealth advisory.
- Asset management.

Chartis focuses on risk and compliance technology, giving it a significant advantage over generic market analysts.

The firm has brought together a leading team of analysts and advisors from the risk management and financial services industries. This team has hands-on experience of developing and implementing risk management systems and programs for Fortune 500 companies and leading consulting firms.

Visit **www.chartis-research.com** for more information.

Join our global online community at **www.risktech-forum.com**.

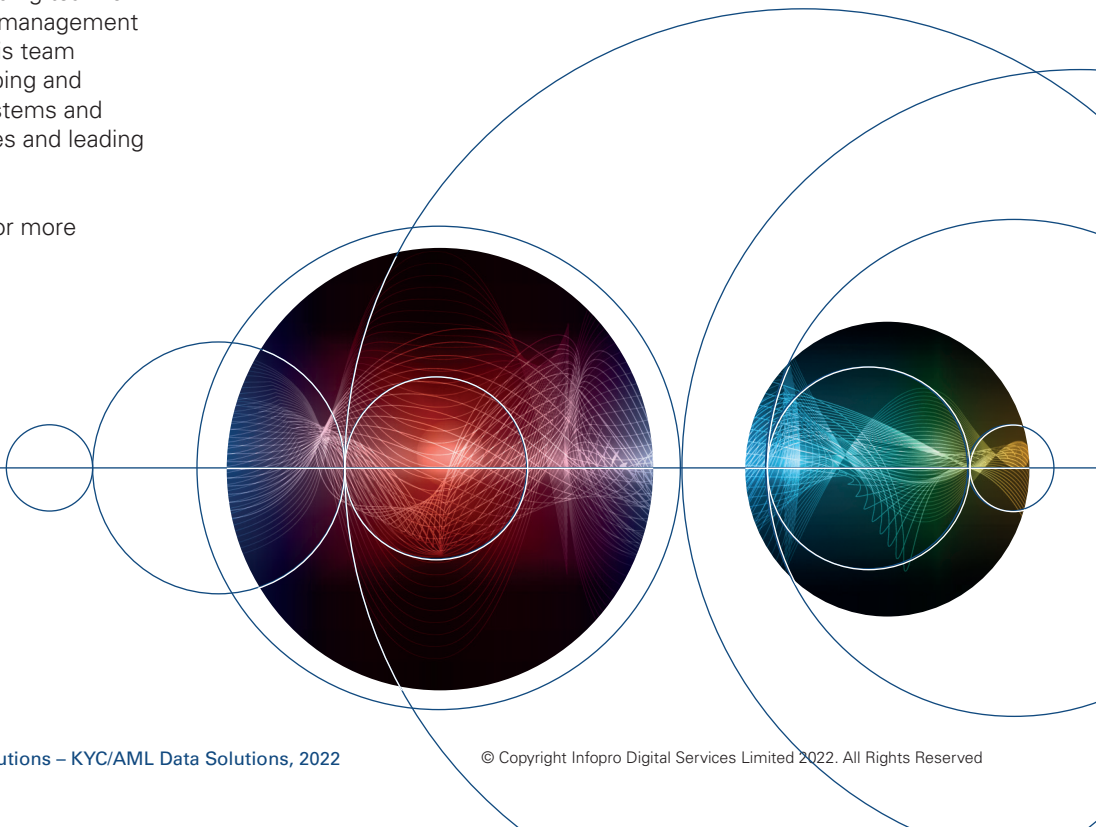


Table of contents

1. Report context 5

2. Quadrant context 7

3. Vendor context 11

4. Methodology 18

5. Further reading 22

List of figures and tables

Figure 1: Market dynamics and data management 5

Figure 2: RiskTech Quadrant® for KYC/AML data solutions, 2022 8

Figure 3: Data resources 13

Figure 4: Enterprise solutions 13

Figure 5: LexID® 14

Figure 6: LexID® Digital 14

Figure 7: Financial Crime Digital Intelligence – managing growing digital sanctions risk 16

Figure 8: Decisioning workflows 16

Figure 9: Customer data management 17

Table 1: Completeness of offering – LexisNexis® Risk Solutions (KYC/AML data solutions, 2022) 9

Table 2: Market potential – LexisNexis® Risk Solutions (KYC/AML data solutions, 2022) 10

Table 3: LexisNexis Risk Solutions – company information 11

Table 4: Evaluation criteria for Chartis' KYC AML data solutions, 2022 report 19

1. Report context

This Vendor Analysis is based on the Chartis quadrant report *KYC/AML Data Solutions, 2022: Market Update and Vendor Landscape* (published in August 2022). This section summarizes the key theses in that report; subsequent sections take a detailed look at the quadrant positioning and scoring for LexisNexis® Risk Solutions, and Chartis' underlying opinion and analysis.

Key thesis

Monitoring the flow of data is a key concern for financial institutions and corporates, and nowhere is this more important than within KYC and AML processes and procedures. Counterparties and individuals are increasingly defined by complex information, at both the corporate and individual levels. In addition, the ways in which individuals are identified and defined have evolved to include information such as addresses, device identities and even biometrics. Financial institutions are now expected to account for the structure and hierarchies of their counterparties (including ultimate beneficial owners [UBOs]), and to record corporate actions.

The ways in which data is used are dictated by two types of requirements:

- **Regulatory requirements**. By law, institutions must know who they are dealing with and perform due diligence on their counterparties.
- **Privacy requirements**. Firms may only be allowed to know limited or specific information about companies and individuals.

These requirements often conflict and depend on regional differences, creating a geographically distinct marketplace for data and data solutions.

While the COVID-19 pandemic no longer dictates market priorities like it did in 2020 and 2021, it has accelerated the demand for data as more financial firms use remote onboarding and identification processes. However, privacy requirements around data have also become more stringent, and this is influencing institutions' responses and technology vendors' strategies.

Against this background, the market for KYC/AML data is in flux. As different use cases or regulatory requirements arise – including more data around trade and the emergence of relatively high-risk businesses (such as cannabis dispensaries in areas where marijuana has been legalized) – related ecosystems of data form around them.

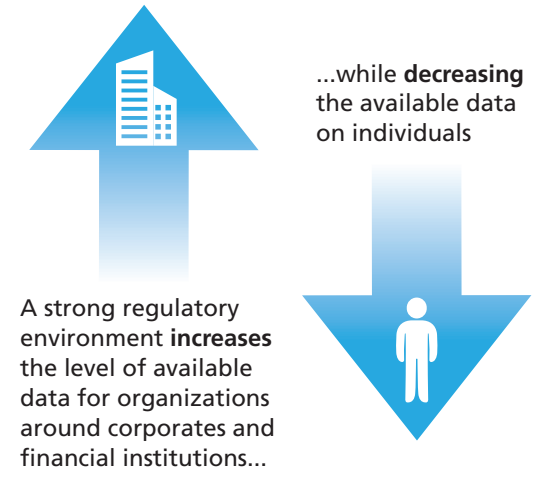
Demand-side takeaways

Context: data and privacy

Financial institutions have a variety of challenges and priorities around data management. Firms have a heightened focus on where and why consumer data is used, and this is informing both institutional and vendor strategies. Several factors are causing this (see Figure 1):

- Increasing regulation.
- More specificity and detail around customer data.
- A stronger focus on individual consumer rights.

Figure 1: Market dynamics and data management



Source: Chartis Research

While institutions have been looking to gain more complete views of individuals and corporate counterparties, they have run afoul of data privacy regulations, which seek to reduce the amount of information an institution can hold on an individual. The tension between these factors has an important impact on the data market. While Europe, for example, has relatively strong data privacy laws, it also requires significant corporate disclosures, and company registry data is relatively

accessible in some European countries. As such, it can be more challenging to access individual or retail data in Europe than in the US.

Managing data privacy regulations – the geography factor

Financial institutions must abide by privacy laws and regulations when conducting KYC checks on clients because of the sensitive personal information being collected during the process. Firms must also be transparent about what happens to the data after it is assessed and used. The European Union's (EU) General Data Protection Regulation (GDPR) has led the way, and compliance among financial institutions has been relatively smooth compared with firms in the corporate sector. This is because financial institutions have comparatively higher levels of governance and consumer data control.

In this context, financial institutions, when managing their data streams, must balance competing priorities:

- **Following different laws**. International companies are required to follow the data privacy laws of the jurisdictions in which they are present.
- **Addressing the cost of data privacy**. For firms, implementing cybersecurity requirements, storing relevant data and ensuring they remain compliant can be costly. There are also costs associated with ensuring that the data transferred to third parties for processing or storing complies with regulations – if breaches are detected, fines can be imposed.

How financial institutions manage these issues depends on the region(s) in which they operate.

The expansion and transformation of the IDV data landscape

As a result of a rise in digital onboarding over the past several years, financial institutions have increased their spending on digital ID verification (IDV) solutions and associated technology. Contributing factors to this rise include:

- **Increased demand during the pandemic**. Financial institutions significantly increased their investments in digital ID solutions to facilitate remote onboarding. Institutions with digital verification solutions are now able to onboard more customers.
- **Security**. Firms need to reassure customers that digital verification is secure, guards against fraud, provides data privacy and is aligned with compliance requirements.
- **Increase in online transactions**. The overall volume of online transactions has risen – again, because of the pandemic. Firms' ability to verify identities online can help to limit fraud.
- **More ways to identify individuals**. These include geolocation, social media accounts, fingerprints, iris scans and/or facial recognition.

The data landscape has changed dramatically as a result of regulatory changes, but many regions also have policies that define the choice of IDV available. The key issue is whether a central ID source exists that can serve as a 'golden source' of truth in a particular region. In essence, this means that:

- If there is a central source of data in a region, vendors must work around it.
- If there isn't, then vendors themselves may be considered the 'golden source'.

The extent to which this is true in different regions varies: all geographies will have something between these two extremes. Increasingly, this will produce a geographically polarized data market, with distinct vendor strategies and technology stacks.

Supply-side takeaways

When examining the vendor landscape, we consider the variety of solutions offered by vendors to help financial institutions meet their KYC/AML data and process issues, and identify some of the challenges vendors themselves face.

Broadly, for initial onboarding and customer analysis, vendors access their data largely through publicly available registries. Different vendors have varying strengths in terms of their geographical coverage.

The point solution and best-of-breed areas of the market are populated by vendors with a core focus on particular datasets. Chartis is seeing a diversification in the geographical focus for data provision: corporate data is no longer a 'global' phenomenon, but one with distinct regional characteristics. Many regional corporate registers are not easily accessible, and some vendors have differentiated themselves from their competitors by providing corporate registries in specific markets such as Europe, the Middle East and Africa (EMEA) and Asia-Pacific.

2. Quadrant context

Introducing the Chartis RiskTech Quadrant®

This section of the report contains:

- The Chartis RiskTech Quadrant® for KYC/AML data solutions, 2022.
- An examination of the featured vendor's positioning and its scores as part of Chartis' analysis.
- A consideration of how the quadrant reflects the broader vendor landscape.

Summary information

What does the Chartis quadrant show?

The RiskTech Quadrant® uses a comprehensive methodology that involves in-depth independent research and a clear scoring system to explain which technology solutions meet an organization's needs. The RiskTech Quadrant® does not simply describe one technology option as the best KYC/AML data solution; rather it has a sophisticated ranking methodology to explain which solutions are best for specific buyers, depending on their implementation strategies.

The RiskTech Quadrant® is a proprietary methodology developed specifically for the risk technology marketplace. It takes into account vendors' product, technology and organizational capabilities. Section 4 of this report sets out the generic methodology and criteria used for the RiskTech Quadrant®.

How are quadrants used by technology buyers?

Chartis' RiskTech® and FinTech™ quadrants provide a view of the vendor landscape in a specific area of risk, financial and/or regulatory technology. We monitor the market to identify the strengths and weaknesses of different solutions and track the post-sales performance of companies selling and implementing these systems. Users and buyers can consult the quadrants as part of their wider research when considering the most appropriate solution for their needs.

Note, however, that Chartis does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Chartis' publications consist of the opinions of its research analysts and should not be construed as statements of fact.

How are quadrants used by technology vendors?

Technology vendors can use Chartis' quadrants to achieve several goals:

- Gain an independent analysis and view of the provider landscape in a specific area of risk, financial and/or regulatory technology.
- Assess their capabilities and market positioning against their competitors and other players in the space.
- Enhance their positioning with actual and potential clients, and develop their go-to-market strategies.

In addition, Chartis' Vendor Analysis reports, like this one, offer insight into specific vendors and their capabilities, with further analysis of their quadrant positioning and scoring.

Chartis Research RiskTech Quadrant® for KYC/AML data solutions, 2022

Figure 2 illustrates Chartis' view of the KYC/AML data vendor landscape, highlighting LexisNexis® Risk Solutions.

Quadrant dynamics

General quadrant takeaways

As in Chartis' previous KYC/AML data research, vendors with strengths across multiple data verticals tend to stand out in the landscape – a dynamic reflected by the high level of mergers and acquisitions in the data market. One key theme reflected in the quadrant is the divergence between retail and corporate data. Note that, given Chartis' historical focus on corporate and investment institutions, we have weighted corporate data capabilities more heavily than those related to retail (individual) data.

Figure 2: RiskTech Quadrant® for KYC/AML data solutions, 2022

Source: Chartis Research

Notably, a strong positive correlation exists between market potential and completeness of offering in the quadrant. This supports the view that the marketplace is driven by strong network effects: as more data is gathered (and/or more discrete data-gathering companies emerge), more profits can be reinvested into gathering more data, creating a virtuous cycle.

All category leaders in the quadrant display strong strategies and integration plans for their data products. While each typically has multiple business products, most have also found ways to integrate these within a commercial framework. Partnerships are also a key theme in the vendor landscape. Many firms, particularly category leaders, provide capabilities to other providers in the market.

Vendor positioning in context – completeness of offering

LexisNexis® Risk Solutions is one of the few vendors that provides capabilities in almost every area of the KYC/AML data marketplace, a differentiator that contributed significantly to its category leader position.

The company provides sanctions and watchlist screening data via its WorldCompliance solution. WorldCompliance helps clients identify individuals and companies linked to more than 50 different risk categories (including money laundering, drug trafficking, terrorist financing, corruption, state-owned entities and politically exposed persons [PEPs]).

The solution contains more than 5 million detailed profiles from across the world. The database content is updated continuously, to help firms quickly identify individuals, organizations and other entities that are linked to more than 60 risk classifications. References to each original source of information are provided within each record. The data collection process (manual or automatic) varies based on the type of data being collected.

The negative news and PEP category was particularly strong for WorldCompliance in our analysis, because LexisNexis Risk Solutions provides its own adverse media solution. This includes enforcement data about individuals who have been arrested, charged, convicted or sentenced for a relevant criminal offense, or who have received disciplinary actions or fines.

WorldCompliance monitors open media sources by going through multiple steps and procedures, to ensure that sources are reputable. It compares publications and articles within major sources and reviews the source's terms of use and privacy policy. It also conducts periodic reviews of existing profiles: in the absence of any alerts, elections, news articles or investigations relating to current entities, all profiles undergo a five-year refresh cycle. (In fact, most profiles are updated before five years.) New information about the solution appears according to the following time frames:

- **Adverse media**. Within seven days of information being available on a reputable open-source outlet.
- **Enforcement**. Within 48 hours of information being available on an enforcement agency's official website.
- **PEPs**. Within seven days of a position being announced/recorded on an official government website.
- **Sanctions list**. Within eight hours of information being made available on a sanction agency's official list.

WorldCompliance also has strong traditional, electronic and digital ID capabilities in the US, with more than 200 million individual profiles. Digital ID is also a particularly strong area for LexisNexis Risk Solutions, because of its ThreatMetrix solution. This enables businesses globally to harness intelligence related to devices, locations, identities and past behaviors, to distinguish between trusted and fraudulent behavior. Traditional ID capabilities are contained within the LexID solution set, which is used to resolve, match and manage information on more than 276 million consumer identities in the US.

Data on corporate structure can also be provided though WorldCompliance, covering corporate relationships and hierarchies for state-owned entities (SOEs), as well as individuals or groups that hold an executive decision-making role in the governing body of an SOE. These individuals include directors and C-level managers, or individuals or groups that hold senior management positions (such as senior executives involved in the day-to-day operations of an SOE).

Table 1 shows Chartis' rankings for the vendor's coverage against each of the completeness of offering criteria.

Table 1: Completeness of offering – LexisNexis® Risk Solutions (KYC/AML data solutions, 2022)

Completeness of offering criterion	Coverage
Sanctions and watchlist data	High
Negative news and PEPs	High
Traditional ID	High
Electronic and digital ID	High
Corporate structure	Medium
Entity resolution	Medium
Data methodology	Medium
High-risk business	Medium

Source: Chartis Research

Vendor positioning in context – market potential

To respond to and stay abreast of an increase in demand for data in multiple industries, including financial services, LexisNexis Risk Solutions has grown its client base and widened its area of focus. It has grown and consolidated its position as a major data business with a specific focus on the retail and digital ID segments, while retaining a significant position in corporate and sanctions data. This breadth of capabilities contributed to its position as a category leader in the Chartis RiskTech® Quadrant.

The company's high ranking for market penetration reflects its large client base, which includes 100 of the Fortune 500; WorldCompliance has a strong presence in the US and internationally. The company has established itself as a leader in data gathering, and its services are used by firms in multiple industries. WorldCompliance has also demonstrated an ability to address and provide data on multiple risk factors.

Table 2 shows Chartis' rankings for the vendor's coverage against each of the market potential criteria.

Table 2: Market potential – LexisNexis® Risk Solutions (KYC/AML data solutions, 2022)

Market potential criterion	Coverage
Customer satisfaction	Medium
Market penetration	High
Growth strategy	Medium
Financials	High

Source: Chartis Research

3. Vendor context

Overview of relevant solutions/ capabilities

As one of the largest risk data aggregators in the US, LexisNexis® Risk Solutions provides customers with data, solutions and tools that combine public and industry-specific content with advanced technology and analytics. These solutions are designed to help users evaluate and predict risk and enhance operational efficiency.

LexisNexis Risk Solutions has customers across a wide range of industries, including insurance, financial services, e-commerce, healthcare and government. Its extensive data assets and advanced analytics enable clients to manage such risks as identity theft, fraud and money laundering to prevent financial crime and insurance and government-benefit scams. The company also:

- Helps those without traditional credit histories obtain access to funds.
- Assists agencies in collecting revenue.
- Enhances research to improve business outcomes for healthcare companies.
- Works with law enforcement to help solve crimes.

LexisNexis Risk Solutions is one of the largest aggregators of data in the US and a leading provider of physical, digital and open-source data to support all areas of the customer lifecycle. In addition, by enabling customers to design and control data-based automated workflows, the company increases the value of its data. Moreover, the company's prevalence in the areas of physical and digital identity verification provides a strong position from which it can start to increase the value of its data for existing customers, via the capabilities offered by portals and platforms.

Table 3 provides a summary of the vendor and its solutions.

Table 3: LexisNexis Risk Solutions – company information

Company	LexisNexis Risk Solutions
Headquarters	1000 Alderman Dr, Alpharetta, GA 30005
Other offices	UK, Singapore, Australia, Brazil
Description	LexisNexis Risk Solutions leverages data and advanced analytics to provide insights to help businesses and government entities reduce risk and improve their decision-making. The company provides data and technology solutions for a wide range of industries, including insurance, financial services, e-commerce, healthcare and government. LexisNexis Risk Solutions is part of RELX (LSE: REL/ NYSE: RELX), a global provider of information and analytics for professional and business customers.
Solution	LexisNexis Risk Solutions offers a suite of KYC solutions, including US and global electronic identity verification (eIDV), document authentication, digital identity, watchlist screening and due diligence data for risk, and compliance and screening managers. Powered by its digital identity, physical identity and public records assets, the company's KYC solutions are made available via its own fraud and financial crime platforms. This enables customers to combine datasets for near real-time decisioning, automate workflows to better identify and mitigate financial crime and drive operational efficiencies. The company's target markets are financial services, capital markets, non-banking financial institutions (NBFIs), manufacturing, logistics, freight, shipping, energy, telecom, media, utilities, travel, hospitality, gaming and other market data-driven organizations.

Source: LexisNexis Risk Solutions

Whether used for Know Your Customer, Know Your Business or Know Your Vendor processes domestically or globally, LexisNexis® Risk Solutions' broad suite of KYC solutions, partners and orchestration platforms can help to transform an organization's fraud and financial crime operations from end to end. The vendor's solutions allow its customers to combine its array of digital identity, physical identity, contributory intelligence, behavioral intelligence, screening data, public records, criminal records, due diligence data and consortium intelligence with other first- and third-party data for near-real-time decisioning within automated, highly efficient workflows.

Underpinned by its proprietary LexID® and LexID® Digital linking technologies, LexisNexis Risk Solutions' broad KYC suite is used by global fraud and financial crime compliance teams of all sizes across a multitude of industries, including insurance, financial services, e-commerce, healthcare, law enforcement, government and more. Its solutions are designed to enable better fraud and financial crime prevention within automated workflows that drive operational efficiencies while delivering a better experience for customers across multiple channels.

eIDV, document authentication and identity management

Verify and validate physical identities or authenticate documents.

- LexisNexis® InstantID®.
- LexisNexis® InstantID® Business.
- LexisNexis® Instant Verify International.
- LexisNexis® TrueID® Document Authentication.
- LexisNexis® Customer Data Management.

Digital identity and behavioral intelligence

Verify that an entity presenting in digital channels is who it says it is.

- LexisNexis® Digital Identity Network®.
- LexisNexis® Emailage®.
- LexisNexis® BehavioSec®.
- LexisNexis® Behavioral Biometrics.

Fraud risk

Better assesses and prevents fraud losses without undue problems and issues.

- LexisNexis® Fraud Intelligence.
- LexisNexis® FraudPoint®.
- LexisNexis® Phone Intelligence.
- LexisNexis® Order Score.

Authentication

Affirms that an entity is, in fact, who it says it is.

- LexisNexis® Knowledge-Based Authentication.
- LexisNexis® Push Authentication.
- LexisNexis® One-Time Password.

Sanctions/watchlist screening

Ensures that business is not being conducted with a sanctioned individual or region.

- LexisNexis® WorldCompliance™ Plus Data.

Due diligence and risk rating

Perform risk rating and investigations with ease.

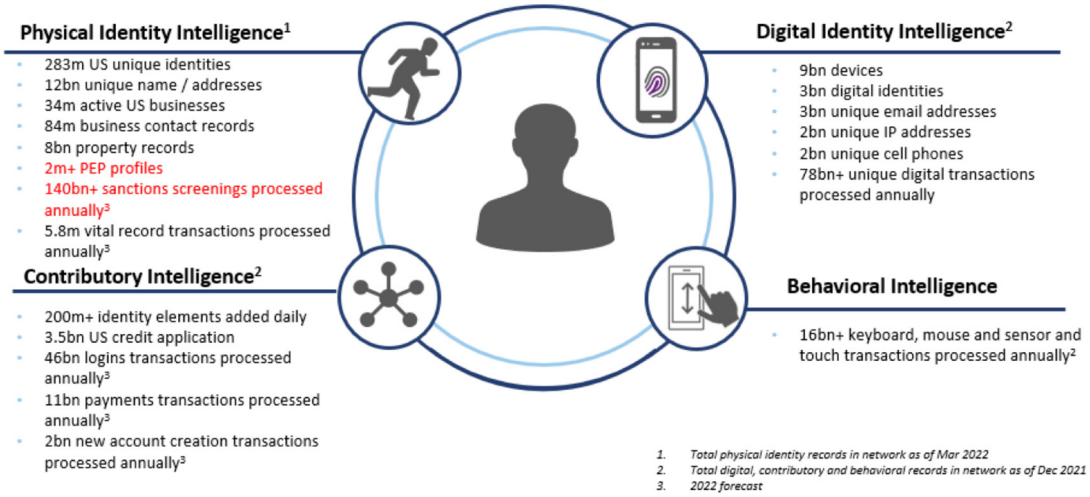
- LexisNexis Risk Management Solutions® and LexisNexis® AML Insight™.
- LexisNexis® Due Diligence Product Suite.
- LexisNexis® Business Assurance Reports.
- Beneficial Ownership.
- LexisNexis® Bankers Almanac® Counterparty KYC.

Fraud and financial crime platforms

Rapidly combine LexisNexis® Risk Solutions and first- and third-party data for near-real-time decisioning within automated workflows.

- LexisNexis® RiskNarrative™.
- LexisNexis® ThreatMetrix®.
- LexisNexis® Dynamic Decision Platform.
- LexisNexis® Financial Crime Digital Intelligence.

Figure 3: Data resources



Source: LexisNexis Risk Solutions

Vendor-leading practices

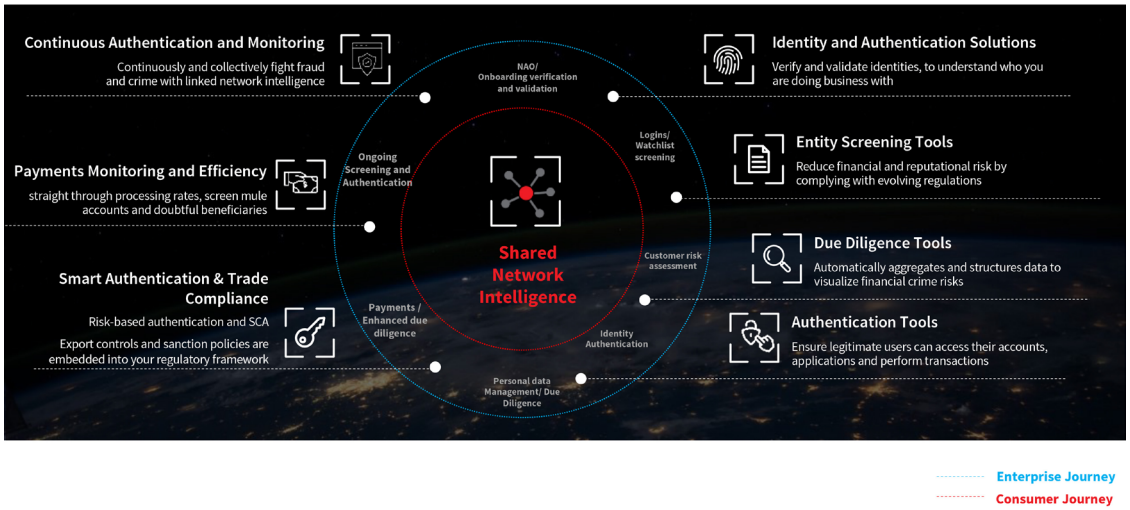
Extensive consumer and business data

The vendor maintains more than 12 petabytes of content that comprises billions of public and proprietary records (see Figure 3).

As one of the leading risk data aggregators in the US, LexisNexis® Risk Solutions is well-positioned to meet an organization's end-to-end KYC needs with its extensive collection of capabilities that cover digital identity, physical identity, contributory intelligence, behavioral intelligence, screening data, public records, criminal records, due diligence data and consortium intelligence.

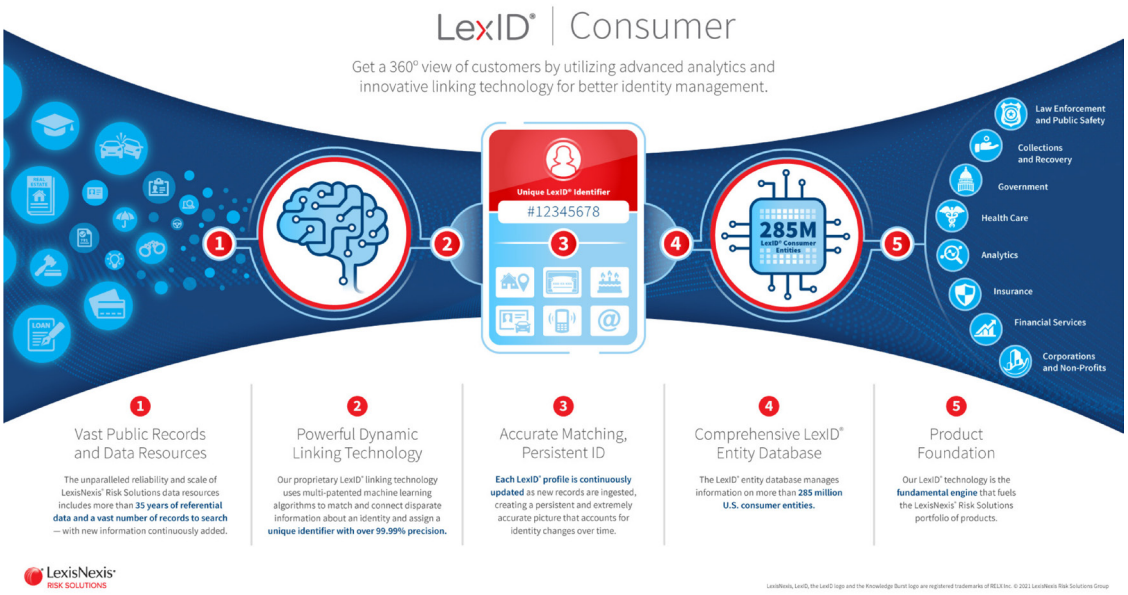
LexisNexis Risk Solutions leverages its leading Big Data computing platform with extensive data assets, proprietary advanced linking technology and a sophisticated analytics platform, to enable businesses of all sizes to turn their data into actionable insights and improve time-to-results and decisions (see Figure 4).

Figure 4: Enterprise solutions



Source: LexisNexis Risk Solutions

Figure 5: LexID®



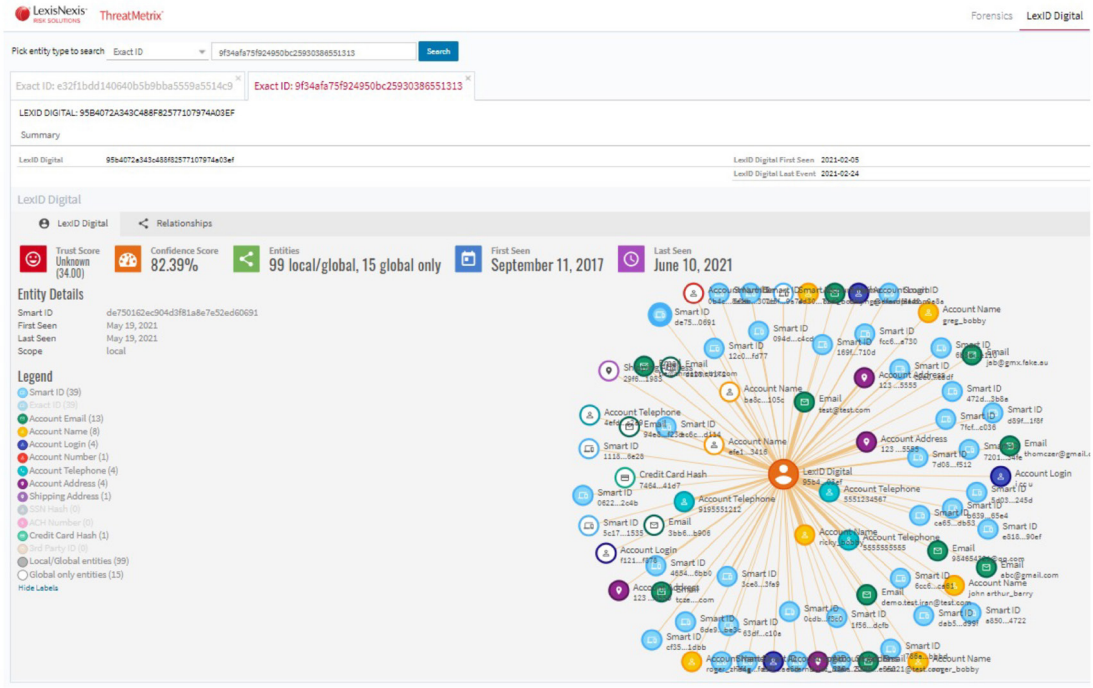
Source: LexisNexis Risk Solutions

LexID® and LexID® Digital

LexisNexis Risk Solutions' proprietary linking technologies, LexID® and LexID® Digital (see Figures 5 and 6), bring together the company's extensive data assets, helping to improve the accuracy of customer data management and provide operational efficiencies within risk processes across the entire customer lifecycle. Key features include:

- **Extensive data**. LexisNexis® Risk Solutions' patented Scalable Automated Linking Technology (SALT) enables the resolution of billions of records into millions of entities, leveraging the data with a high degree of precision and recall.
- **Big Data technology**. The company has a leading open-source Big Data technology platform for data management.

Figure 6: LexID® Digital



Source: LexisNexis Risk Solutions

- **Advanced proprietary linking**. Substantial volumes of data and complex problems can be processed quickly, with 99+% precision for consumer linking and 98+% for businesses.

An extensive suite of KYC solutions available via minimal integrations

LexisNexis Risk Solutions' extensive suite of KYC solutions (detailed previously), combined with the capabilities of its fraud and financial crime platforms, allow its customers to craft end-to-end KYC processes with minimal investment in technical integrations. This has several benefits, helping to ensure that solutions can come to market more quickly, providing effective fraud and financial crime risk management, and helping to enable lower total cost of ownership and substantial operational efficiencies.

Fraud and financial crime platforms

LexisNexis® Risk Solutions' fraud and financial crime platforms provide feature-rich low/no-code, natural language policy creation. This can rapidly combine any of the vendor's KYC solutions with first- and third-party data for near-real-time decisioning across the fraud and compliance consumer, business and vendor lifecycles.

LexisNexis® RiskNarrative™

The RiskNarrative™ platform intelligently orchestrates the customer experience while detecting and preventing financial crime and fraud. The platform simplifies customer onboarding, monitors transactions, helps reduce risk and combats financial crime with a sophisticated, configurable, easy-to-implement customer lifecycle management solution. The RiskNarrative™ platform enables full financial crime compliance management within a single, unified platform with no-code configuration and rapid integration through one easy and intuitive application programming interface (API), orchestrating customer journeys and enabling a single view of customer risk.

LexisNexis® ThreatMetrix®

LexisNexis® ThreatMetrix® is a global enterprise solution for digital identity intelligence and digital authentication, and is used by leading global brands to inform daily transaction decisions. By combining digital identity insights built from billions of transactions with leading analytics technology and embedded machine learning, the vendor's solutions unify decision analytics across the entire customer lifecycle to help:

- Accelerate conversions and maximize revenue.
- Improve transaction security and refine personalization.
- Minimize friction and reduce false positives.
- Reduce abandoned transactions with online payment fraud detection.
- Detect and prevent more fraud.

This end-to-end decisioning platform enables firms to keep valuable transactions in motion while maximizing the effectiveness of critical fraud defenses and cybersecurity risk management processes.

LexisNexis® Dynamic Decision Platform

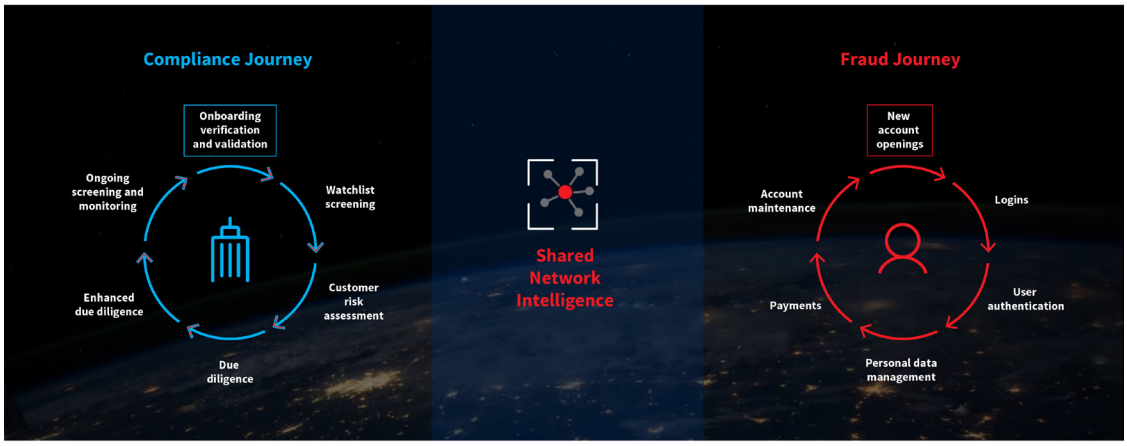
Dynamic Decision Platform incorporates behavioral analytics, machine learning, workflow and orchestration, case management and integration capabilities to help businesses make the best trust decisions across the lifecyle of the customer. Key features include:

- **Behavioral analytics (ThreatMetrix® Smart Rules)**. Advanced behavioral analytics rules that enable firms to gain a better understanding of legitimate user behavior and detect genuine fraud more accurately.
- **Machine learning (ThreatMetrix® Smart Learning)**. A 'clear-box' approach to machine learning that integrates digital identity intelligence with Smart Rules to produce optimized models with fewer false positives.
- **Workflow and orchestration**. The ability to integrate external data sources into the ThreatMetrix® decision engine and access pre-integrated third-party services for transactions that require additional assurance/exception handling.
- **Case management**. Helps firms to optimize authentication and fraud decisions by monitoring, updating and isolating transactions that require additional review. This helps to give firms a smarter, more integrated way to handle increasingly complex caseloads with shrinking resources.

LexisNexis® Financial Crime Digital Intelligence on ThreatMetrix®

Financial Crime Digital Intelligence is a compliance solution, purpose-built for digital financial crime, which leverages the shared global digital identity and location intelligence provided by LexisNexis® ThreatMetrix®. Financial Crime Digital Intelligence

Figure 7: Financial Crime Digital Intelligence – managing growing digital sanctions risk



Source: LexisNexis Risk Solutions

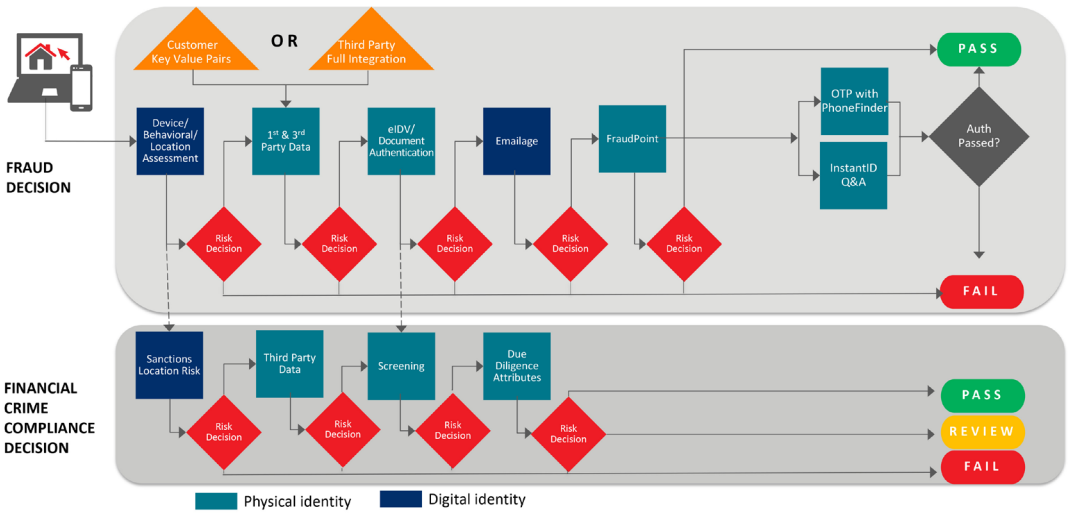
(see Figure 7) helps businesses better identify true sanctions risk in near-real time, using custom-designed policies and automated workflows that match their risk appetite. Financial Crime Digital Intelligence makes it possible for financial crime compliance teams to:

- **Better detect digital sanctions evasion and unmask potential evaders** (who may be attempting to obfuscate their true location with technologies such as proxy, VPN or TOR browser) with Sanctions Location Risk. This leverages insights from those entities' prior behavior across the LexisNexis® Digital Identity Network®.
- **Call in real time for a match to a sanctions list** with Sanctions List Match.
- **Combine digital identity and location intelligence** with traditional financial crime data to create near-real-time decisioning and automated workflows that drive new efficiencies.
- **Speed up investigations and meet emerging regulatory requirements** related to digital identity and location, using dynamic identity visualization tools and forensic reporting.

With robust workflow orchestration capabilities, LexisNexis® Risk Solutions' customers can quickly and easily incorporate policies for near-real-time decisioning within self-designed fraud and financial crime automated workflows, waterfalling to multiple pre-integrated KYC solutions and seamlessly triggering subsequent actions.

These **Decisioning Workflows** can help firms vet the identity of a business, individual, identity credential or device to prevent or investigate fraudulent transactions and/or improve operational efficiency (see Figure 8).

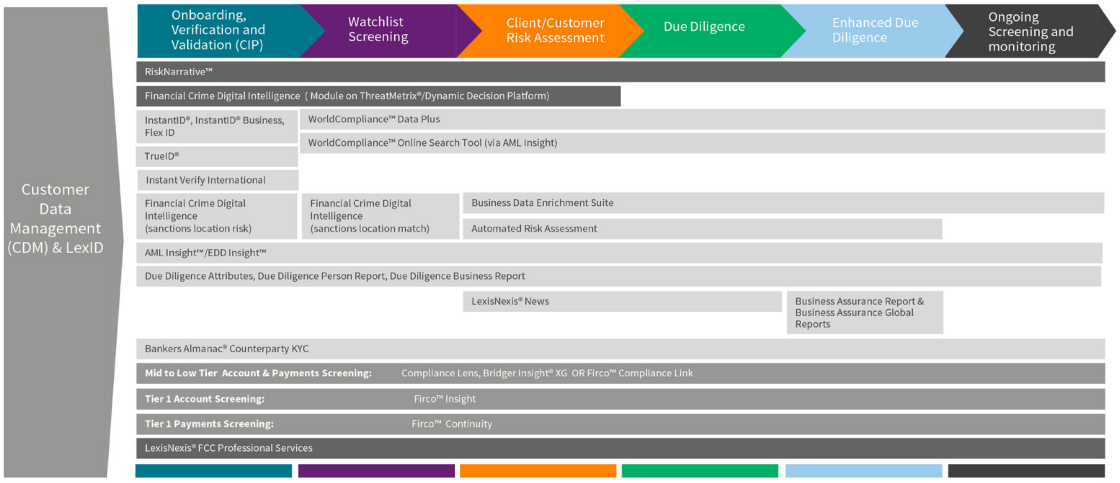
Figure 8: Decisioning workflows



Source: LexisNexis Risk Solutions

As a result, the vendor's customers can improve operational efficiencies, better detect and manage fraud and financial crime risk across the customer lifecycle, and design elegant customer journeys, enabling users to transact with more trust and confidence (see Figure 9).

Figure 9: Customer data management



Source: LexisNexis Risk Solutions

4. Methodology

Overview

Chartis is a research and advisory firm that provides technology and business advice to the global financial services industry. Chartis provides independent market intelligence regarding market dynamics, regulatory trends, technology trends, best practices, competitive landscapes, market sizes, expenditure priorities, and mergers and acquisitions. Chartis' RiskTech® and FinTech™ quadrant reports are written by experienced analysts with hands-on experience of selecting, developing and implementing financial technology solutions for a variety of international companies in a range of industries, including banking, insurance and capital markets. The findings and analyses in our quadrant reports reflect our analysts' considered opinions, along with research into market trends, participants, expenditure patterns and best practices.

Chartis seeks to include RiskTech and FinTech vendors that have a significant presence in a given target market. The significance may be due to market penetration (e.g., a large client base) or innovative solutions. Chartis uses detailed vendor evaluation forms and briefing sessions to collect information about each vendor. If a vendor chooses not to respond to a Chartis request for information, Chartis may still include the vendor in the report. Should this happen, Chartis will base its opinion on direct data collated from technology buyers and users, and from publicly available sources.

Chartis' research clients include leading financial services firms and Fortune 500 companies, leading consulting firms and financial technology vendors. The vendors evaluated in our quadrant reports can be Chartis clients or firms with whom Chartis has no relationship.

Chartis evaluates all vendors using consistent and objective criteria, regardless of whether they are Chartis clients. Chartis does not give preference to its own clients and does not request compensation for inclusion in a quadrant report, nor can vendors influence Chartis' opinion.

Briefing process

We conducted face-to-face and/or web-based briefings with each vendor1. During these sessions, Chartis experts asked in-depth, challenging questions to establish the real strengths and weaknesses of each vendor. Vendors provided Chartis with:

- A business update – an overview of solution sales and client satisfaction.
- A product update – an overview of relevant solutions and R&D roadmaps.
- A product demonstration – key differentiators of their solutions relative to those of their competitors.

In addition to briefings, Chartis used other third-party sources of data, such as conferences, academic and regulatory studies, and publicly available information.

Evaluation criteria

We develop specific evaluation criteria for each piece of quadrant research from a broad range of overarching criteria, outlined below. By using domain-specific criteria relevant to each individual risk, we can ensure transparency in our methodology, and allow readers to fully appreciate the rationale for our analysis. The specific criteria used for KYC AML data solutions are shown in Table 4.

Completeness of offering

- **Depth of functionality**. The level of sophistication and number of detailed features in the software product (e.g., advanced risk models, detailed and flexible workflow, domain-specific content). Aspects assessed include innovative functionality, practical relevance of features, user-friendliness, flexibility and embedded intellectual property. High scores are given to firms that achieve an appropriate balance between sophistication and user-friendliness. In addition, functionality linking risk to performance is given a positive score.
- **Breadth of functionality**. The spectrum of requirements covered as part of an enterprise risk management system. This varies for each subject area, but special attention is given to functionality covering regulatory requirements, multiple risk classes, multiple asset classes,

[1] *Note that vendors do not always respond to requests for briefings; they may also choose not to participate in the briefings for a particular report.*

Table 4: Evaluation criteria for Chartis' KYC AML data solutions, 2022 report

Completeness of offering	Market potential
• Sanctions and watchlist data	• Customer satisfaction
• Negative news and PEPs	• Market penetration
• Traditional ID	• Growth strategy
• Electronic and digital ID	• Financials
• Corporate structure	
• Entity resolution	
• Data methodology	
• High-risk business	

Source: Chartis Research

multiple business lines and multiple user types (e.g., risk analyst, business manager, CRO, CFO, compliance officer). Functionality within risk management systems and integration between front-office (customer-facing) and middle/back office (compliance, supervisory and governance) risk management systems are also considered.

- **Data management and technology infrastructure**. The ability of risk management systems to interact with other systems and handle large volumes of data is considered very important. Data quality is often cited as a critical success factor and ease of data access, data integration, data storage and data movement capabilities are all important factors. Particular attention is given to the use of modern data management technologies, architectures and delivery methods relevant to risk management (e.g., in-memory databases, complex event processing, component-based architectures, cloud technology and Software as a Service). Performance, scalability, security and data governance are also important factors.

- **Risk analytics**. The computational power of the core system, the ability to analyze large amounts of complex data in a timely manner (where relevant in real time) and the ability to improve analytical performance are all important factors. Particular attention is given to the difference between 'risk' analytics and standard 'business' analytics. Risk analysis requires such capabilities as non-linear calculations, predictive modeling, simulations, scenario analysis, etc.

- **Reporting and presentation layer**. The ability to present information in a timely manner, the quality and flexibility of reporting tools, and their ease of use, are important for all risk management systems. Particular attention is given to the ability to do ad hoc 'on-the-fly' queries (e.g., 'what-if' analysis), as well as the range of 'out of the box' risk reports and dashboards.

Market potential

- **Business model**. Includes implementation and support and innovation (product, business model and organizational). Important factors include size and quality of implementation team, approach to software implementation, and post-sales support and training. Particular attention is given to 'rapid' implementation methodologies and 'packaged' services offerings. Also evaluated are new ideas, functionality and technologies to solve specific risk management problems. Speed to market, positioning and translation into incremental revenues are also important success factors in launching new products.

- **Market penetration**. Volume (i.e., number of customers) and value (i.e., average deal size) are considered important. Rates of growth relative to sector growth rates are also evaluated. Also covers brand awareness, reputation and the ability to leverage current market position to expand horizontally (with new offerings) or vertically (into new sectors).

- **Financials**. Revenue growth, profitability, sustainability and financial backing (e.g., the ratio of license to consulting revenues) are considered key to scalability of the business model for risk technology vendors.

- **Customer satisfaction**. Feedback from customers is evaluated, regarding after-sales support and service (e.g., training and ease of implementation), value for money (e.g., price to functionality ratio) and product updates (e.g., speed and process for keeping up to date with regulatory changes).

- **Growth strategy**. Recent performance is evaluated, including financial performance, new product releases, quantity and quality of contract wins, and market expansion moves. Also considered are the size and quality of the sales force, sales distribution channels, global presence, focus on risk management, messaging and positioning. Finally, business insight and understanding, new thinking, formulation and execution of best practices and intellectual rigor are considered important.

Quadrant construction process

Chartis constructs its quadrants after assigning scores to vendors for each component of the completeness of offering and market potential criteria. By aggregating these values, we produce total scores for each vendor on both axes, which are used to place the vendor on the quadrant.

Definition of quadrant boxes

Chartis' quadrant reports do not simply describe one technology option as the best solution in a particular area. Our ranking methodology is designed to highlight which solutions are best for specific buyers, depending on the technology they need and the implementation strategy they plan to adopt. Vendors that appear in each quadrant have characteristics and strengths that make them especially suited to that particular category, and by extension to particular users' needs.

Point solutions

- Point solutions providers focus on a small number of component technology capabilities, meeting a critical need in the risk technology market by solving specific risk management problems with domain-specific software applications and technologies.
- They are often strong engines for innovation, as their deep focus on a relatively narrow area generates thought leadership and intellectual capital.
- By growing their enterprise functionality and utilizing integrated data management, analytics and business intelligence (BI) capabilities, vendors in the point solutions category can expand their completeness of offering, market potential and market share.

Best-of-breed

- Best-of-breed providers have best-in-class point solutions and the ability to capture significant market share in their chosen markets.
- They are often distinguished by a growing client base, superior sales and marketing execution, and a clear strategy for sustainable, profitable growth. High performers also have a demonstrable track record of R&D investment, together with specific product or 'go-to-market' capabilities needed to deliver a competitive advantage.
- Because of their focused functionality, best-of-breed solutions will often be packaged together as part of a comprehensive enterprise risk technology architecture, co-existing with other solutions.

Enterprise solutions

- Enterprise solution providers typically offer risk management technology platforms, combining functionally rich risk applications with comprehensive data management, analytics and BI.
- A key differentiator in this category is the openness and flexibility of the technology architecture and a 'toolkit' approach to risk analytics and reporting, which attracts larger clients.
- Enterprise solutions are typically supported with comprehensive infrastructure and service capabilities, and best-in-class technology delivery. They also combine risk management content, data and software to provide an integrated 'one stop shop' for buyers.

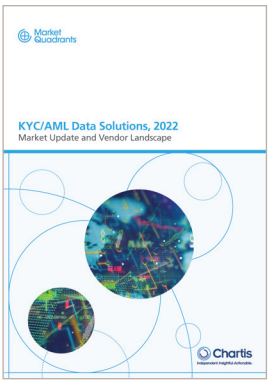
Category leaders

- Category leaders combine depth and breadth of functionality, technology and content with the

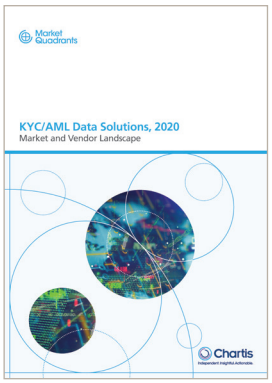
required organizational characteristics to capture significant share in their market.

- They demonstrate a clear strategy for sustainable, profitable growth, matched with best-in-class solutions and the range and diversity of offerings, sector coverage and financial strength to absorb demand volatility in specific industry sectors or geographic regions.
- They will typically benefit from strong brand awareness, a global reach and strong alliance strategies with leading consulting firms and systems integrators.

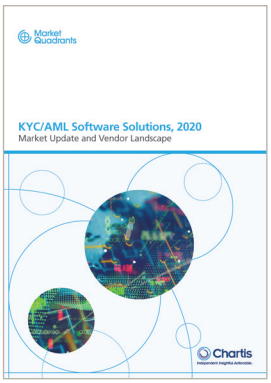
5. Further reading



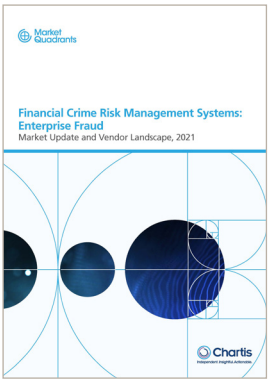
KYC/AML Data Solutions, 2022: Market Update and Vendor Landscape



KYC/AML Data Solutions, 2020: Market and Vendor Landscape



KYC/AML Software Solutions, 2020: Market Update and Vendor Landscape



Financial Crime Risk Management Systems: Enterprise Fraud; Market Update and Vendor Landscape, 2021

Big Bets 2022

RiskTech100® 2022

For all these reports, see **www.chartis-research.com**